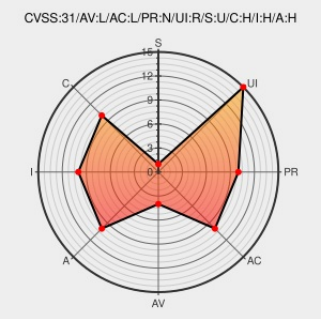
# CVE-2016-5330

Published on: 08/07/2016 12:00:00 AM UTC

Last Modified on: 11/05/2021 04:33:00 PM UTC

## CVE-2016-5330

Source: Mitre | Source: NIST | CVE.ORG | Print: PDF




Certain versions of Mac Os X from Apple contain the following vulnerability:

Untrusted search path vulnerability in the HGFS (aka Shared Folders) feature in VMware Tools 10.0.5 in VMware ESXi 5.0 through 6.0, VMware Workstation Pro 12.1.x before 12.1.1, VMware Workstation Player 12.1.x before 12.1.1, and VMware Fusion 8.1.x before 8.1.1 allows local users to gain privileges via a Trojan horse DLL in the current working directory.

CVE-2016-5330 has been assigned by cve@mitre.org to track the vulnerability - currently rated as HIGH severity.

### CVSS3 Score: 7.8 - HIGH

| Attack Vector | Attack Complexity | Privileges Required | User Interaction |
|---|---|---|---|
| LOCAL | LOW | NONE | REQUIRED |
| **Scope** | **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| UNCHANGED | HIGH | HIGH | HIGH |

### CVSS2 Score: 4.4 - MEDIUM

| Access Vector | Access Complexity | Authentication |
|---|---|---|
| LOCAL | MEDIUM | NONE |
| **Confidentiality Impact** | **Integrity Impact** | **Availability Impact** |
| PARTIAL | PARTIAL | PARTIAL |

### CVE References

| Description | Tags | Link |
|---|---|---|
| VMware ESXi Server Header | www.securitytracker.com text/html | SECTRACK 1036544 |

| | | |
|---|---|---|
| Injection Flaw Lets Remote Users Conduct Cross-Site Scripting and Redirect Attacks and DLL Loading Error Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker | | |
| DLL side loading vulnerability in VMware Host Guest Client Redirector | securify.nl<br>text/html | MISC securify.nl/advisory/SFY20151201/dll_side_loading_vulnerability_in_vmware_host_guest_client_r |
| SecurityFocus | www.securityfocus.com<br>text/html | BUGTRAQ 20160805 DLL side loading vulnerability in VMware Host Guest Client Redirector |
| VMware Tools CVE-2016-5330 DLL Loading Remote Code Execution Vulnerability | cve.report (archive)<br>text/html | BID 92323 |
| VMSA-2016-0010.1 | Mitigation<br>Vendor Advisory<br>www.vmware.com<br>text/html | CONFIRM www.vmware.com/security/advisories/VMSA-2016-0010.html |
| VMware DLL Loading Error Lets Remote Users Execute Arbitrary Code on the Target System - SecurityTracker | www.securitytracker.com<br>text/html | SECTRACK 1036545 |
| DLL Side Loading Vulnerability in VMware Host Guest Client Redirector | www.rapid7.com<br>text/html | MISC www.rapid7.com/db/modules/exploit/windows/misc/vmhgfs_webdav_dll_sideload |
| VMware vRealize Log Insight Lets Remote Users Traverse the Directory to View Files on the Target System - SecurityTracker | www.securitytracker.com<br>text/html | SECTRACK 1036619 |

By selecting these links, you may be leaving CVEreport webspace. We have provided these links to other websites because they may have information that would be of interest to you. No inferences should be drawn on account of other sites being referenced, or not, from this page. There may be other websites that are more appropriate for your purpose. CVEreport does not necessarily endorse the views expressed, or concur with the facts presented on these sites. Further, CVEreport does not endorse any commercial products that may be mentioned on these sites. Please address comments about any linked pages to comment@cve.report.

There are currently no QIDs associated with this CVE

## Known Affected Configurations (CPE V2.3)

| Type | Vendor | Product | Version | Update | Edition | Language |
|---|---|---|---|---|---|---|
| Operating System | Apple | Mac Os X | - | All | All | All |
| Operating System | Microsoft | Windows | - | All | All | All |
| Operating System | Vmware | Esxi | 5.0 | All | All | All |
| Operating System | Vmware | Esxi | 5.1 | All | All | All |
| Operating System | Vmware | Esxi | 5.5 | All | All | All |
| Operating System | Vmware | Esxi | 6.0 | All | All | All |
| Operating System | Vmware | Esxi | 5.0 | All | All | All |
| Operating System | Vmware | Esxi | 5.1 | All | All | All |
| Operating System | Vmware | Esxi | 5.5 | All | All | All |
| Operating System | Vmware | Esxi | 6.0 | All | All | All |
| Operating System | Vmware | Esxi | All | All | All | All |
| Application | Vmware | Fusion | All | All | All | All |
| Application | Vmware | Fusion | 8.1 | All | All | All |
| Application | Vmware | Fusion | 8.1 | All | All | All |
| Application | Vmware | Fusion | 8.1.1 | All | All | All |
| Application | Vmware | Fusion | 8.1 | All | All | All |
| Application | Vmware | Fusion | 8.1 | All | All | All |
| Application | Vmware | Fusion | 8.1.1 | All | All | All |
| Application | Vmware | Tools | 10.0.5 | All | All | All |
| Application | Vmware | Tools | 10.0.5 | All | All | All |
| Application | Vmware | Tools | All | All | All | All |
| Application | Vmware | Workstation Player | All | All | All | All |

| | | | | | | |
|---|---|---|---|---|---|---|
| Application | Vmware | Workstation Player | 12.1 | All | All | All |
| Application | Vmware | Workstation Player | 12.1.1 | All | All | All |
| Application | Vmware | Workstation Player | 12.1 | All | All | All |
| Application | Vmware | Workstation Player | 12.1.1 | All | All | All |
| Application | Vmware | Workstation Pro | All | All | All | All |
| Application | Vmware | Workstation Pro | 12.1 | All | All | All |
| Application | Vmware | Workstation Pro | 12.1.1 | All | All | All |
| Application | Vmware | Workstation Pro | 12.1 | All | All | All |
| Application | Vmware | Workstation Pro | 12.1.1 | All | All | All |

cpe:2.3:o:apple:mac_os_x:-:*:*:*:*:*:*:*:

cpe:2.3:o:microsoft:windows:-:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.5:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.0:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.1:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:5.5:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:6.0:*:*:*:*:*:*:*:

cpe:2.3:o:vmware:esxi:*:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:*:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:8.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:8.1:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:vmware:fusion:8.1.1:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:vmware:fusion:8.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:fusion:8.1:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:vmware:fusion:8.1.1:*:*:*:*:mac_os_x:*:*:

cpe:2.3:a:vmware:tools:10.0.5:*:*:*:*:windows:*:*:

cpe:2.3:a:vmware:tools:10.0.5:*:*:*:*:windows:*:*:

cpe:2.3:a:vmware:tools:*:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_player:*:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_player:12.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_player:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_player:12.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_player:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_pro:*:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_pro:12.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_pro:12.1.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_pro:12.1:*:*:*:*:*:*:*:

cpe:2.3:a:vmware:workstation_pro:12.1.1:*:*:*:*:*:*:*:

No vendor comments have been submitted for this CVE

← Previous ID

Next ID→